bmc

Solution White Paper

A Holistic Approach to BMC Product Security

BMC Product Security Team

Table of Contents

Product security at BMC

BMC develops enterprise software across multiple geographies, using multiple technologies and development methodologies. Our enterprise software solutions are summarized at https://www.bmc.com/it-solutions/digital-enterprise-management.html.

Scope of the Product Security Program

The Product Security Program described here applies to BMC enterprise software solutions focused on service management and IT operations management. All BMC products maintained by Digital Service Management and Digital Service Operations must achieve quality certification before they are released. Digital Service Management products include the BMC Helix product family. Digital Service Operations products include the TrueSight product family. Quality certification is issued only when a product, including all its components and dependencies, meets the relevant security requirements.

Responsibility for the Product Security Program

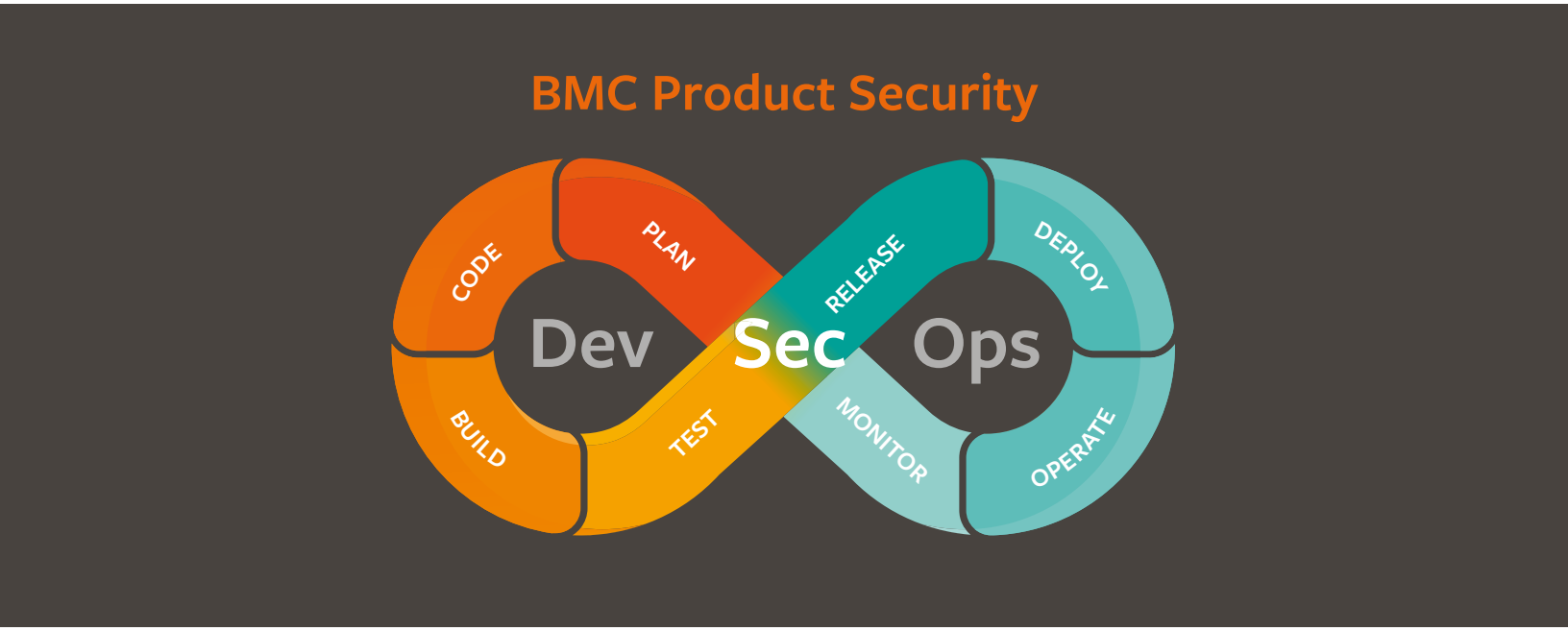
Each product line at BMC is responsible for all aspects of their offerings, including development lifecycles, quality, technical support, and sales and marketing support.

The Product Security Team at BMC is responsible for upholding BMC corporate standards of quality, especially as those standards relate to defining, evangelizing, and measuring all aspects of security within all product line development lifecycles.

At BMC, product security is considered to be an integral aspect of product quality.

Continuous improvement of the Product Security Program

Security is a journey rather than an end goal or a final state. Our security practices are always evolving. We adapt our tools and techniques to encompass new technologies and protect against new kinds of threats.



PRODUCT SECURITY CONTACT

For security-related inquiries, please email appsec@bmc.com.

If you have questions about a particular product, please contact your account or sales team.

OVERVIEW

BMC products must meet security-related standards defined by BMC before they can be released and throughout their Secure Software Development Lifecycle (SSDLC). Security standards apply to both the developmental and operational phases. BMC has a governing policy, metrics, and guidelines for ensuring that all BMC products meet these standards.

This document provides details of security considerations through the SSDLC of a BMC product. The SSDLC begins with a product's initial conception and design and follows the product through development, testing, delivery, and operation. The Product Security Program describes how BMC uses a "build-security-in" model at every stage of software development and operations.

SECURE SOFTWARE DEVELOPMENT LIFECYCLE

BMC treats security as an integral part of the software development life cycle. By using an agile SSDLC process, BMC is able to address security at each phase of the software development lifecycle. Security tools and processes are most effective when integrated throughout the SSDLC, as opposed to only considered at the end of the development process. According to US-CERT, "the cost of correction of security flaws at the requirements level is up to 100 times less than the cost of correction of security flaws in fielded software."[1]

BMC incorporates threat modeling, attack surface analysis, security architecture analysis, and other techniques at early phases of application conception. Developers use a "shift-left" approach to security. Beginning with early phases of development, developers incorporate tools for security assessments, threat modeling, security testing, and penetration testing. Software is designed to follow industry best practices, including least privilege, failing securely, defense in depth, and separation of privilege.

We incorporate security techniques such as threat modeling, attack surface analysis, and security architecture analysis.

QUALITY CERTIFICATION

BMC products that are subject to this Product Security Program must achieve quality certification before they are released. Security signoff for quality certification is issued only when a product, including all its components and dependencies, meets the relevant security requirements.

BMC products

Depending on its nature, each product must go through Dynamic Application Security Testing (DAST), manual penetration testing, or both.

- DAST is performed using industry-leading testing tools. These tools analyze applications in their dynamic, running state during the testing phase of the product development lifecycle. They simulate attacks against an application and analyze the application's response. The analysis shows whether the product is vulnerable, especially against the OWASP Top 10[2] most critical web application security risks.
- Manual penetration testing is performed at BMC by the internal penetration-testing team, external penetration-testing companies, or both.

If these procedures identify any high-severity vulnerabilities (CVSS v3 score higher than 7.0), the development team corrects those vulnerabilities before releasing the product.

1 US-CERT Estimating Benefits from Investing in Secure Software Development, https://www.us-cert.gov/bsi/articles/knowledge/business-case-models/estimating-benefits-from-investing-in-secure-software-development

2 OWASP Top 10 2017, The Top Ten Critical Web Application Security Risks, https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

External software and dependencies

If a BMC product depends upon third-party or open-source software and components, quality certification for that product requires a security vulnerability review, performed using an industry-leading vulnerability-scanning engine.

- For third-party software, a manual review is performed.
- For each open-source software component and library, an automated scan against the National Vulnerability Database is performed to identify any known vulnerabilities in the specific version used in a BMC product.

All findings of the security vulnerability review are rated according to the Common Vulnerability Scoring System (CVSS v3) and handled according to their severity. Before the product is released, all high-severity vulnerabilities[3] are patched or upgraded. Medium- and low-severity vulnerabilities[4] are analyzed for relevance and logged to be addressed in later releases if they are not remediated in the current release.

MALWARE PREVENTION

To reduce the risk of introducing malicious code or malware into BMC products, the following measures are in place at BMC:

- Peer code reviews are conducted prior to source code check-in and product builds. This mechanism is enforced via the quality certification process.
- Dynamic Application Security Testing is enforced via the quality certification process.
- All product environments must meet corporate information security requirements. These requirements include endpoint protection, which is deployed on all build servers and engineering clients

MANUAL APPLICATION PENETRATION TESTING

Manual application penetration testing is performed annually, independently of the quality review for every major release of BMC software. After the product development group trains them on the product's business functionality and architecture, the Application Security Team, a sub-group of the Product Security Team, performs penetration testing. Penetration testing comprises system-level tests, web application tests (including an enhanced checklist based on OWASP Top 10 Security Vulnerabilities[5]), client-server tests, API tests, and network scanning. Depending on the findings, security design discussions might also be required. BMC also often engages third-party firms to conduct manual penetration testing and independently identify vulnerabilities in our products.

PRODUCT SECURITY CONSULTING

In addition to coordinating quality certification, malware prevention, and penetration testing, the Product Security Team provides security-related consulting services to all product development groups. Typical consulting engagements include security design reviews, architectural advice, and security implementation advice. We also offer guidance on the use of security scanning tools and the interpretation of their results.

The Product Security Team provides security-related consulting services to all product development groups.

3 NIST Information Technology Laboratory National Vulnerability Database Common Vulnerability Scoring System Calculator Version 3, https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

4 NIST Information Technology Laboratory National Vulnerability Database Vulnerability Metrics, https://nvd.nist.gov/vuln-metrics/cvss

5 OWASP Top 10 Security Vulnerabilities, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

SECURE DEVELOPMENT EDUCATION

BMC has partnered with an industry-leading security training firm to provide a corporate-wide training plan for the education of all developers, QA engineers, product managers, and architects. The plan includes mandatory training on the OWASP Top 10 Security Vulnerabilities.

Security training is customized for specific job descriptions:

- Developers (C/C++, Java, Web development languages such as JavaScript and Ruby)
- QA Engineers (testing web applications and thick client applications)
- Architects (security design, threat modeling)
- Product Managers (security requirement definitions, threat modeling)
- Executives (application security overview)

To date, more than 550 developers at BMC have undergone training on the first three domains of the ISC[2] Certified Secure Software Lifecycle Professional (CSSLP) secure coding program. CSSLP certification recognizes application security experts who can incorporate security practices into each phase of the software development lifecycle. Some of these developers have achieved the ISC[2] Secure Software Practitioner (SSP) certification.[6] SSP certification recognizes professionals who are prepared to develop secure software and enhance our overall security posture. Because so many of our development team members have achieved or are pursuing these security-focused certifications, BMC is thoroughly prepared to continue creating and maintaining secure software.

SECURITY DESIGN REVIEWS AND THREAT MODELING

Automated tools and penetration testing rarely discover design flaws in business logic. To add security-focused human insight, the BMC Product Security Team conducts design reviews and threat modeling workshops. This enables us to identify and address potential security flaws during the architecture phase of product development.

SECURITY RESPONSE AND COMMUNICATION

- The Product Security Team maintains the BMC Security web page at https://www.bmc.com/corporate/product-security-and-quality.html. The web page includes contact information, a public PGP key, security news, and the procedure followed for vulnerability disclosure by third parties such as security researchers.
- Product vulnerabilities disclosed by third parties such as security researchers are handled following the procedure described at https://www.bmc.com/corporate/product-security-and-quality.html.
- Publicly-disclosed vulnerabilities in third-party and open-source software components embedded within or shipped with BMC products can affect multiple product lines. When such vulnerabilities are discovered, the Product Security Team orchestrates efforts across product lines to assess the risk to BMC products. The team also communicates the availability of fixes or workarounds via the BMC support news site at https://communities.bmc.com/blogs/application-security-news.
- The Product Security site at https://communities.bmc.com/blogs/application-security-news provides all kinds of security-related information, not just news of specific vulnerabilities.
- The Product Security Team follows a formal escalation process for vulnerability disclosures regardless of their source (researcher, customer, internal QA team, or others). Based on the severity of the vulnerability, it is routed through senior management, remediated by the relevant product development team, and communicated to affected customers by the product support team.

Incident management

The Product Security Team at BMC uses an incident management procedure that enables swift response to any potential incident. This incident management procedure is integrated within the overall corporate cyber incident response plan. This procedure covers emergency incidents, escalation, and public vulnerability disclosure. BMC practices include a procedure for documenting the incident in detail and producing a report for future reference or management attention.

Cloud-hosted applications

BMC products are increasingly being developed to be hosted in cloud environments. These environments include Amazon Web Services (AWS) as well as the BMC cloud. BMC has specific security policies to address BMC products in the cloud.

6 ISC2 Secure Software Practitioner Certificate, https://www.isc2.org/Training/Secure-Software-Practitioner-Suites

CERTIFICATIONS

The BMC Helix Remedy environment, hosted by BMC, achieved FedRAMP and SOC2 certification. Some products adhere to FIPS, PCI, or STIG guidelines. Some products adhere to the CIS AWS security benchmarks. Other products are in the planning or testing phases of achieving certifications.

PRODUCT SECURITY CONTACT

For security-related inquiries, please email **appsec@bmc.com**.

About BMC

BMC helps customers run and reinvent their businesses with open, scalable, and modular solutions to complex IT problems. Bringing both unmatched experience in optimization and limitless passion for innovation to technologies from mainframe to mobile to cloud and beyond, BMC helps more than 10,000 customers worldwide reinvent, grow, and build for the future success of their enterprises.

BMC—the multi-cloud management company. **www.bmc.com**

bmc

508463